

MICROSOFT 365 PDF / ANONYMIZED APP-DERIVED EXCERPT

Approved tenant evidence - Microsoft 365 excerpt

ANONYMIZED APP-DERIVED EXCERPT - Selected and edited from an existing assessment. Identifiers and private values are removed. This is not an unmodified report, a complete assessment or a customer-results claim.

Origin and edition

First-party test assessment. Authenticated exports of existing stored assessments from the current SCOUTz app. No new scan was run for this sample review.

Selected and edited excerpts from the app's cloud executive client report and client AI report. This is not one original unmodified report and does not certify readiness.

Observed October 7, 2026 / Display alias: example.com

example.com is a reserved display alias replacing the reviewed domain. These observations were not collected from example.com. No replacement application, user or DNS values are invented.

Scope and coverage limits

Supported configuration, application inventory and metadata observed through customer-approved tenant access. This does not imply access to message bodies, files, chats, documents, prompts or actual AI-agent activity.

Source: Cloud executive client report, p. 1 / Observed October 7, 2026

Full collector reads were incomplete or unconfirmed. The report expressly distinguishes retained records and individual reads from confirmed complete collector coverage.

These are the unread states actually present in the selected exports. They do not declare each whole area unread. Missing counts or omitted areas do not establish complete coverage or a clean result.

Actual unread checks and scope restrictions are retained on page 4. These excerpts do not certify organizational or Copilot readiness.

Identity and application context

Selected first-party test evidence. Source, date and limits stay with each observation.

Administrator authentication methods need review

Cloud executive client report, p. 2 / Observed October 7, 2026

Cloud executive finding - authentication review

Observed evidence: The report identifies administrator authentication methods as needing review.

Uncertainty and limits: The excerpt does not expose account identities, underlying methods or effective policy details. This title is not a conclusion about every administrator or proof of compromise.

Proposed next check: Verify account purpose, registered methods, effective policies and recent sign-ins. Preserve tested emergency access when staging any approved change.

AI-related application inventory

Client AI report, p. 1 / Observed October 7, 2026

Observed Microsoft 365 application inventory

Observed evidence: AI-related applications appear in the retained Microsoft 365 inventory.

Uncertainty and limits: Ownership or registration does not establish business approval, granted permissions or actual use. This inventory is not complete Shadow IT discovery or runtime inspection.

Proposed next check: Ask each business owner to confirm purpose and approval. Verify supported permissions and relevant activity evidence separately before recommending access changes.

Permissions and consent context

Selected first-party test evidence. Source, date and limits stay with each observation.

Permission evidence and data-use limits

Client AI report, p. 6 / Observed October 7, 2026

Retained connected-app inventory and supported permission metadata

Observed evidence: The report records data-related permission or privilege indicators for AI-related applications.

Uncertainty and limits: Permission does not prove effective access or actual data use, and these inputs do not link an AI app to a particular shared file. Zero listed signals does not establish complete coverage.

DLP policy posture is not readable under the granted scopes - a visibility gap, not a clean result.

Proposed next check: Validate consent, delegated or application permission scope, resource restrictions and business need with the owner. Review external sharing separately and confirm DLP coverage.

Application-consent policy observation

Client AI report, p. 1 / Observed October 7, 2026

Observed application-consent policy

Observed evidence: App-consent control: user consent is restricted by the observed policy.

Uncertainty and limits: A policy observation does not establish that all existing grants are appropriate or that every application use is approved.

Proposed next check: Review the intended consent process, existing grants and accountable owners against the organization's approved policy.

Unread checks stay unknown

Actual read limitations in the selected cloud executive and client AI reports. The states below describe checks and scope restrictions, not a whole-area verdict.

Identity & Access

Cloud executive client report, p. 1 / Observed October 7, 2026

Contains checks reported as not read

Perimeter

Cloud executive client report, p. 1 / Observed October 7, 2026

Contains checks reported as not read

DLP policy posture

Client AI report, p. 6 / Observed October 7, 2026

Not readable under the granted scopes

These are the unread states actually present in the selected exports. They do not declare each whole area unread. Missing counts or omitted areas do not establish complete coverage or a clean result.

Cloud executive client report, p. 3 / Observed October 7, 2026

Not read means an attempted check could not be confirmed; an omitted area is not certified.

Keep the next decision separate

Keep observations, customer-confirmed context, documented gaps and questions not assessed separate. Review the permission reference, methodology and pricing before an open-beta application.

The source exports are combined only for this edited excerpt. Neither omitted evidence nor an application inventory establishes active use, complete coverage or a readiness verdict.

[Review methodology](#) / [Review pricing](#) / [Apply for open beta](#)